(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年9 月26 日 (26.09.2002)

PCT

(10) 国際公開番号
WO 02/076016 A1

(51) 国際特許分類[7]: H04L 9/38, H04B 10/20

(21) 国際出願番号: PCT/JP02/02672

(22) 国際出願日: 2002 年3 月20 日 (20.03.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-081501 2001 年3 月21 日 (21.03.2001) JP

(71) 出願人 (米国を除く全ての指定国について): 科学技術振興事業団 (JAPAN SCIENCE AND TECHNOLOGY CORPORATION) [JP/JP]; 〒332-0012 埼玉県 川口市本町４丁目１番８号 Saitama (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 竹内 繁樹 (TAKEUCHI,Shigeki) [JP/JP]; 〒005-0004 北海道 札幌市 南区澄川４条１丁目２−５ ガーデン胡桃Ｂ２０２ Hokkaido (JP).

(74) 代理人: 西澤 利夫 (NISHIZAWA,Toshio); 〒150-0042 東京都 渋谷区 宇田川町３７−１０ 麻仁ビル６階 Tokyo (JP).

(81) 指定国 (国内): AU, CA, NO, US.

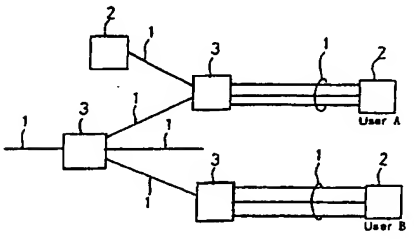
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

[続葉有]

(54) Title: QUANTUM CIPHER COMMUNICATION SYSTEM

(54) 発明の名称: 量子暗号通信システム



(57) Abstract: A quantum cipher communication system for quantum cipher communication in an optical network. The system comprises a transmitter for transmitting a packet signal having at least an light pulse train representing an address and a single photon pulse train used for quantum cipher, and a router including a header analyzer for extracting the address information in the light pulse train from the packet signal and a gate switch for selecting one of optical fibers. The router routes the packet signal by selecting an optical fiber used for the next transmission path according to the extracted address information by the header analyzer and by switching the path to the selected optical fiber by the gate switch.

(57) 要約:

光ネットワークにおいて量子暗号通信を行う量子暗号通信システムであって、少なくともアドレスを表す光パルス列および量子暗号で用いる単一光子パルス列を有するパケット信号を発信する送信機と、前記パケット信号から光パルス列のアドレス情報を検出するヘッダアナライザおよび各光ファイバへの切換えを行うゲートスイッチを有するルータとを備えており、ルータは、ヘッダアナライザによる検出アドレス情報に基づいて次の送信路となる光ファイバを選択し、ゲートスイッチによりその光ファイバへの切換えを行って、パケット信号をルーティングする。

WO 02/076016 A1

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書
量子暗号通信システム

技術分野

この出願の発明は、量子暗号通信システムに関するものである。さらに詳しくは、この出願の発明は、光ネットワークにおける多対多での鍵配送を実現することのできる、新しい量子暗号通信システムに関するものである。

背景技術

近年、共通鍵方式のＤＥＳ暗号（Data Encryption Standard 暗号）や公開鍵方式のＲＳＡ暗号（Rivest-Shamir-Adleman 暗号）などに取って代わる次世代の暗号技術として、量子暗号が注目されており、研究・開発が盛んに進められている。この量子暗号を用いた情報通信は、遠距離の２者間で他者に知られることなく秘密鍵を共有することを可能とする。

しかしながら、これまでに開発されている量子暗号通信技術はいずれも、特定の固定された回線を用いた１対１、もしくは１対多での鍵配送を前提としており、これでは光ネットワーク上にて量子暗号通信を行おうとした場合、各ユーザ毎に専用の光ファイバを設置しなければならないなど、光ネットワーク上での実用化には好ましいものでなかった。

そこで、この問題を解決すべく、ビームスプリッタによって信号分配する方法が既に提案されている（特表平９－５０２３２０号参照）。しかしながら、この方法では送信者から多数のユーザに鍵がランダムに分配されるので、ユーザ数Ｎにしたがってその鍵配送レートが１／Ｎに減少してしまうといった問題があった。

この出願の発明は、以上のとおりの事情に鑑みてなされたものであり、従来技術の問題点を解消し、光ネットワーク内のあるユーザから別の特定のユーザに向けて鍵共有を行うことを可能とし、多対多での鍵配送を実現することのできる、新しい量子暗号通信システムを提供することを課題としている。

発明の開示

この出願の発明は、上記の課題を解決するものとして、光ファイバにより構成される光ネットワークにおいて量子暗号通信を行う量子暗号通信システムであって、少なくともアドレスを表す光パルス列および量子暗号で用いる単一光子パルス列を有するパケット信号を発信する送信機と、前記パケット信号から光パルス列のアドレス情報を検出するヘッダアナライザおよび各光ファイバへの切換えを行うゲートスイッチを有するルータとを備えており、ルータは、ヘッダアナライザによる検出アドレス情報に基づいて次の送信路となる光ファイバを選択し、ゲートスイッチによりその光ファイバへの切換えを行って、パケット信号をルーティングすることを特徴とする量子暗号通信システムを提供する。

図面の簡単な説明

図１は、この出願の発明の量子暗号通信システムの全体構成を例示した図である。

図２は、この出願の発明の量子暗号通信システムにおけるパルス信号を例示した図である。

図３は、この出願の発明の量子暗号通信システムにおけるルータの内部構成を例示した図である。

なお、図中の符号は次のものを示す。

１　光ファイバ
２　送信機
３　ルータ
３１　ヘッダアナライザ
３２　ゲートスイッチ

発明を実施するための最良の形態

この出願の発明は、上記のとおりの特徴を有するものであるが、以下にその実施の形態について説明する。

図１～図３は、各々、この出願の発明の量子暗号通信システムを

説明する図であり、図１は光ファイバ（１）により構成される光ネットワーク上に送信機（２）およびルータ（３）を備えたこの出願の発明の量子暗号通信システムの全体構成を例示したもの、図２はパルス信号を例示したもの、図３はルータ（３）の内部構成を例示したものである。

たとえばこれら図１～図３に例示したように、この出願の発明では、少なくともアドレスを表す光パルス列および量子暗号で用いる単一光子パルス列を有するパケット信号を発信する送信機（２）と、送信機（２）により送られてきたパケット信号から光パルス列のアドレス情報を検出するヘッダアナライザ（３１）および各光ファイバ（１）への切換えを行うゲートスイッチ（３２）を有するルータ（３）とを備えている。

そして、ルータ（３）は、ヘッダアナライザ（３１）による検出アドレス情報に基づいて次の送信路となる光ファイバ（１）を選択し、ゲートスイッチ（３２）によりその光ファイバ（１）への切換えを行って、パケット信号をルーティングする。これにより、単一光子パルス列を含むパケット信号は、ルータ（３）を通る度に適切な光ファイバ（１）へ伝達されていく。

すなわち、この出願の発明の量子暗号通信システムは、パケット通信的な手法によって、量子暗号で用いる単一光子列を、ルーティングにより、光ネットワーク内のあるＵｓｅｒＡから特定のＵｓｅｒＢをはじめとする多数のユーザへ送信することができるのである。したがって、たとえば光ファイバが引かれた各家庭から基地局などへ量子暗号を用いた通信が可能となり、量子暗号を一般家庭でも使用でき、多対多の量子暗号通信が実現されるようになる。

送信機（２）は、たとえば、図示していないが量子暗号手段、パケット信号作成手段およびパケット信号発信手段を有しており、量子暗号手段による量子暗号の単一光子パルス列をパケット信号作成手段によってパケット信号に分割し、各パケット信号毎にアドレスを表すヘッダとなる光パルス列を付加した後、パケット信号発信手段によりそのパケット信号を接続されている光ファイバー（１）へ送る。光ファイバー（１）により構成される光ネットワーク上に

は複数のルータ（３）が設けられており、各ルータ（３）間にてパケット信号のルーティングが行われる。

図２に例示したパケット信号では光パルス列および単一光子パルス列は時間的に分割されているが、ルータ（３）のヘッダアナライザ（３１）によってアドレス情報を検出できる限り、これらが混在していても、あるいは異なる周波数に分割されていてもよい。ヘッダアナライザ（３１）によるアドレス情報検出には、公知のパケット通信にて用いられている各種手法を用いることができる。

また、光パルス列については、アドレス（送信先ＩＰアドレスなど）を表すヘッダのみでなく、たとえば通常の古典的な通信で使用するための信号パルスをも含むものとすることができる。

またさらに、ルータ（３）については、全光学スイッチによる構成も可能であり、この場合では、光パルス列（ヘッダ部分）の光非線型性によって一定時間ゲートスイッチ（３２）が開き、その間に単一光子パルス列を含むパケット信号が次の光ファイバ（１）へ伝達されることになる。

もちろん、この発明は以上の例に限定されるものではなく、細部については様々な態様が可能である。

産業上の利用可能性

以上詳しく説明した通り、この出願の発明によって、光ネットワーク内のあるユーザから別の特定のユーザに向けて鍵共有を行うことを可能とし、多対多での量子暗号通信を実現することのできる、新しい量子暗号通信システムが提供される。

請求の範囲

1．光ファイバにより構成される光ネットワークにおいて量子暗号通信を行う量子暗号通信システムであって、

少なくともアドレスを表す光パルス列および量子暗号で用いる単一光子パルス列を有するパケット信号を発信する送信機と、

前記パケット信号から光パルス列のアドレス情報を検出するヘッダアナライザおよび各光ファイバへの切換えを行うゲートスイッチを有するルータとを備えており、

ルータは、ヘッダアナライザによる検出アドレス情報に基づいて次の送信路となる光ファイバを選択し、ゲートスイッチによりその光ファイバへの切換えを行って、パケット信号をルーティングすることを特徴とする量子暗号通信システム。

図 1

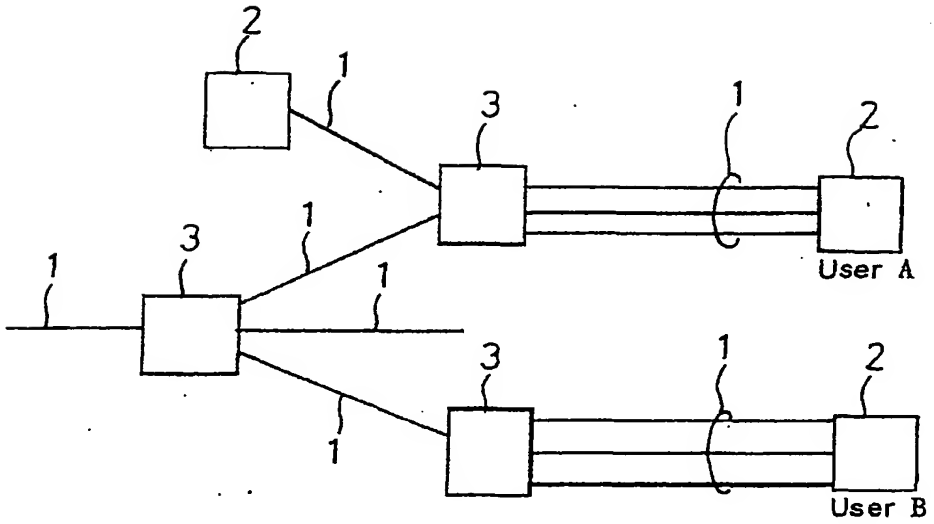


図 2

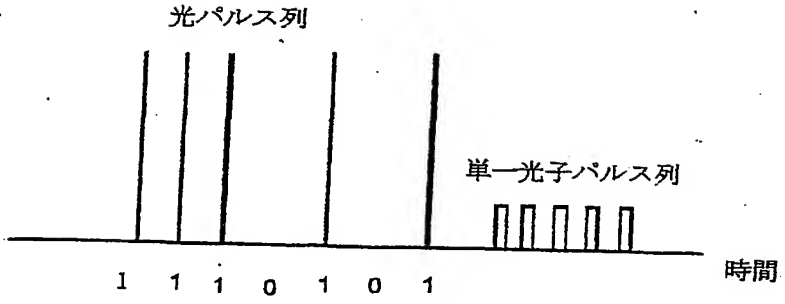
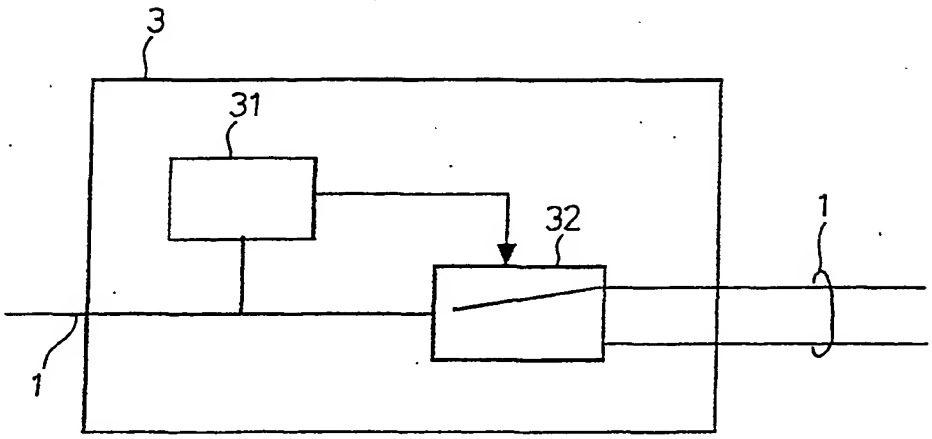


図 3



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/02672

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/38, H04B10/20

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/38, H04B10/20

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2002
Kokai Jitsuyo Shinan Koho	1971-2002	Jitsuyo Shinan Toroku Koho	1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 6-261073 A (Nippon Telegraph And Telephone Corp.), 16 September, 1994 (16.09.94), Full text; Figs. 1 to 5 (Family: none)	1

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 01 May, 2002 (01.05.02)	Date of mailing of the international search report 21 May, 2002 (21.05.02)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０２／０２６７２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／３８，Ｈ０４Ｂ１０／２０

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷　Ｈ０４Ｌ９／３８，Ｈ０４Ｂ１０／２０

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００２年
日本国登録実用新案公報	１９９４－２００２年
日本国実用新案登録公報	１９９６－２００２年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ　６－２６１０７３　Ａ（日本電信電話株式会社） １９９４．０９．１６　全文，図１－５　（ファミリーなし）	１

☐ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ０１．０５．０２	国際調査報告の発送日　21.05.02
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） 青木　重徳　　５Ｍ　４２２９ 電話番号　０３－３５８１－１１０１　内線　３５９７

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）